

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000215108 A

(43) Date of publication of application: 04.08.00

(51) Int. Cl

G06F 12/14

G06F 15/78

H01L 27/115

H01L 21/8247

H01L 29/788

H01L 29/792

(21) Application number: 11014458

(71) Applicant: TOSHIBA CORP

(22) Date of filing: 22.01.99

(72) Inventor: KASAI HISAMICHI

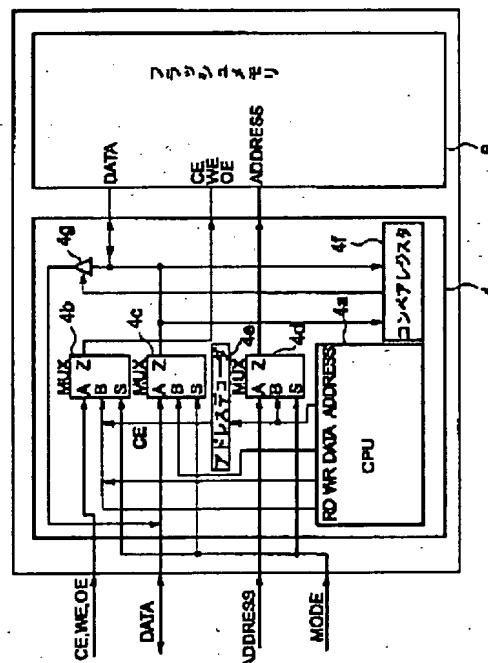
(54) SEMICONDUCTOR INTEGRATED CIRCUIT

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a semiconductor integrated circuit which can provide a security function for a memory chip in the semiconductor integrated circuit having an MCP formed by mounting a memory chip and a CPU chip on one package.

SOLUTION: In a semiconductor circuit(MCP) having the flash memory chip 6 and CPU chip 4 mounted on one package, a signature code read out of the flash memory chip 6 and a security resetting data inputted from an outside are compared by a comparison register 4f. Only when they match each other, a tri-state buffer 4g enables the flash memory chip 6 to be read.

COPYRIGHT: (C)2000,JPO



Best Available Copy

Best Available Copy

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-215108
(P2000-215108A)

(43)公開日 平成12年8月4日(2000.8.4)

(51) Int.Cl. ⁷	識別記号	F I	テーコード(参考)
G 06 F 12/14	3 2 0	G 06 F 12/14	3 2 0 C 5 B 0 1 7
15/78	5 1 0	15/78	5 1 0 C 5 B 0 6 2
H 01 L 27/115		H 01 L 27/10	5 1 0 F 5 F 0 0 1
21/8247		29/78	4 3 4 5 F 0 8 3
			3 7 1

審査請求 未請求 請求項の数 3 OL (全 5 頁) 最終頁に続く

(21)出願番号 特願平11-14458

(22)出願日 平成11年1月22日(1999.1.22)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 萩原 央倫

神奈川県川崎市幸区堀川町580番1号 株式会社東芝半導体システム技術センター内

(74)代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5B017 AA03 BA01 BA09 BB03 CA11

CA12

5B062 AA07 CC01 DD10 EE09

5F001 AG40 AH10

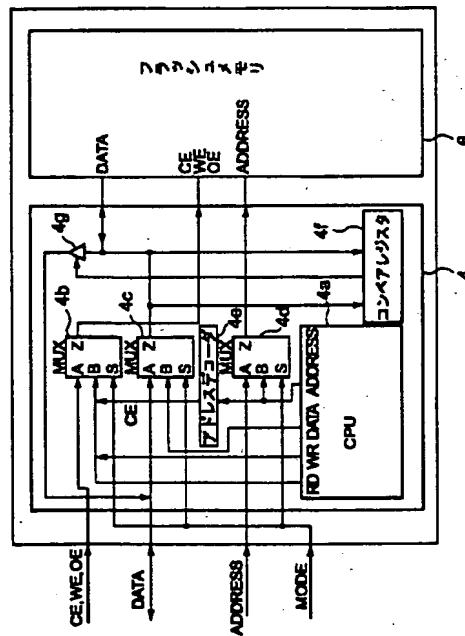
5F083 ER21 GA30 ZA12 ZA13 ZA23

(54)【発明の名称】 半導体集積回路

(57)【要約】

【課題】メモリチップとCPUチップを1つのパッケージに実装してMCPを形成した半導体集積回路において、メモリチップに対してセキュリティ機能を設けることができる半導体集積回路を提供する。

【解決手段】フラッシュメモリチップ6とCPUチップ4とを1つのパッケージに実装した半導体集積回路(MCP)において、フラッシュメモリチップ6から読み出したシグネチャコードと、外部から入力されたセキュリティ解除用データとがコンペアレジスタ4fにより比較される。そして、コンペアレジスタ4fによる比較結果が一致した場合のみ、トライステイトバッファ4gによってフラッシュメモリチップ6に対する読み出しが許可される。



【特許請求の範囲】

【請求項1】 不揮発性メモリチップとロジックICチップを1つのパッケージに実装した半導体集積回路(MCP)において、

前記不揮発性メモリチップに予め記憶された参照用データと外部から入力された照合用データを比較する比較手段と、

前記比較手段による比較結果に応じて、前記不揮発性メモリチップに記憶されたデータの読み出しを許可あるいは禁止する許可手段と、

を具備することを特徴とする半導体集積回路。

【請求項2】 パッケージに実装され、第1のデータを記憶する不揮発性メモリチップと、外部から入力される第2のデータと前記第1のデータとを比較する比較手段と、

前記比較手段による比較結果に応じて、前記不揮発性メモリチップに記憶されたデータの読み出しを許可あるいは禁止する許可手段と、

前記比較手段と前記許可手段を有し、前記不揮発性メモリチップが実装されたパッケージと同一のパッケージに実装されたロジックICチップと、

を具備することを特徴とする半導体集積回路。

【請求項3】 前記ロジックICチップは、MPU(マイクロプロセッサ)、CPUあるいはMCU(メモリコントロールユニット)であることを特徴とする請求項1または2のいずれかに記載の半導体集積回路。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、半導体集積回路のセキュリティに関し、特に不揮発性メモリチップとMPU(マイクロプロセッサ)チップ等を同一のパッケージに実装した半導体集積回路(MCP)のセキュリティに関するものである。

【0002】

【従来の技術】 近年、基板及び実装技術の進歩により、MCP(Multi Chip Package)やMCM(Multi Chip Module)と呼ばれる、複数のチップを1つのパッケージに実装(1パッケージ化)する技術が開発されている。

【0003】 このMCPのメリットとしては、まず開発の容易さを挙げることができる。既存のチップをわずかな修正で様々なチップと1パッケージ化できることより、製品開発を容易に行うことができる。また、プロセス的にも有効であり、不揮発性メモリチップとMPUチップ(あるいはCPU(Central Processing Unit)チップ、MCU(Memory Control Unit)チップ)を1パッケージ化したMCPのケースで考えると、メモリーロジック混載技術が不要になるなど、様々なメリットが考えられる。

【0004】

【課題】 しかし、上記の技術問題に対しては、不揮発性メモリ(以下、NVメモリ)チップとCPUチップを1パッケージ化したMCPを例に取り、その課題を説明する。

【0005】 例えば、NVメモリチップを他社開発汎用品、CPUチップを既存自社開発品とする。この場合、CPUチップに対してNVメモリチップのI/Fを付加しMCP化すると、NVメモリチップの仕様が理解できるユーザが利用した場合、このNVメモリチップに対してのセキュリティ機能が働かなくなってしまう。

【0006】 そこでこの発明は、前記課題に鑑みてなされたものであり、メモリチップとCPUチップを1つのパッケージに実装してMCPを形成した半導体集積回路において、CPUチップのわずかな変更により、メモリチップに対してセキュリティ機能を設けることができる半導体集積回路を提供することを目的とする。

【0007】

【課題を解決するための手段】 前記目的を達成するためには、この発明に係る半導体集積回路は、不揮発性メモリチップとロジックICチップを1つのパッケージに実装した半導体集積回路(MCP)において、前記不揮発性メモリチップに予め記憶された参照用データと外部から入力された照合用データを比較する比較手段と、前記比較手段による比較結果に応じて、前記不揮発性メモリチップに記憶されたデータの読み出しを許可あるいは禁止する許可手段とを具備することを特徴とする。

【0008】 また、この発明に係る半導体集積回路は、不揮発性メモリチップとロジックICチップを1つのパッケージに実装した半導体集積回路(MCP)において、前記不揮発性メモリチップに予め記憶された参照用データと外部から入力された照合用データを比較する比較手段と、前記比較手段による比較結果が一致したとき前記不揮発性メモリチップに記憶されたデータの読み出しを許可し、一致しないとき前記データの読み出しを禁止する手段とを具備することを特徴とする。

【0009】 また、この発明に係る半導体集積回路は、パッケージに実装され、第1のデータを記憶する不揮発性メモリチップと、外部から入力される第2のデータと前記第1のデータとを比較する比較手段と、前記比較手段による比較結果に応じて、前記不揮発性メモリチップに記憶されたデータの読み出しを許可あるいは禁止する許可手段と、前記比較手段と前記許可手段を有し、前記不揮発性メモリチップが実装されたパッケージと同一のパッケージに実装されたロジックICチップとを具備することを特徴とする。

【0010】 また、この発明に係る半導体集積回路は、不揮発性メモリチップとロジックICチップを1つのパッケージに実装した半導体集積回路(MCP)において、前記不揮発性メモリチップに予め記憶されたシグネチャコードと外部から入力された照合用データを比較する比較手段と、前記比較手段による比較結果が一致したとき前記データの読み出しを許可する許可手段とを具備することを特徴とする。

とき前記不揮発性メモリチップに記憶されたデータの読み出しを許可し、比較結果が一致しないとき前記不揮発性メモリチップに記憶されたデータの読み出しを禁止する手段とを具備することを特徴とする。

【0011】

【発明の実施の形態】以下、図面を参照してこの発明の実施の形態の半導体集積回路について説明する。以下の実施の形態では、CPUが形成されたCPUチップとフラッシュメモリが形成されたフラッシュメモリチップを、1つのパッケージに実装してMCP (Multi Chip Package)とした場合を例として説明する。

【0012】図1は、この発明の実施の形態のMCPの外観を示す概略図である。なお、この図では、パッケージ上を被覆する前の状態を示している。

【0013】図1に示すように、基板2上には、CPUが形成されたCPUチップ4と、フラッシュメモリが形成されたフラッシュメモリチップ6が実装されている。

【0014】CPUチップ4上にはパッド8が配置され、フラッシュメモリチップ6上にはパッド10が配置されている。基板2の周辺部には外部接続用のパッド12が配置され、CPUチップ4とフラッシュメモリチップ6との間にはこれらを接続するために用いるパッド14が配置されている。そして、CPUチップ4上のパッド8と外部接続用のパッド12との間、フラッシュメモリチップ6上のパッド10と外部接続用のパッド12との間、及びCPUチップ4とフラッシュメモリチップ6間のパッド14間には、これらを電気的に接続するボンディングワイヤ16が形成されている。

【0015】次に、この発明の実施の形態のMCPの構成について説明する。

【0016】図2は、この発明の実施の形態のMCPのブロックダイヤグラムを示す図である。なおここでは、フラッシュメモリチップは、セキュリティ機能を持たない汎用品とする。

【0017】MCPには、CPUチップ4、フラッシュメモリチップ6、及び第1～第4の外部端子が設けられている。CPUチップ4内には、CPU4a、マルチプレクサ(以下MUX)4b～4d、アドレスデコーダ4e、コンペアレジスタ4f、トライステートバッファ4gが設けられている。第1外部端子からは“CE、WE、OE”が入力され、第2外部端子からは“DATA”が入力される。第3外部端子からは“ADDRESS”が入力され、第4外部端子からは“MODE”が入力される。

【0018】まず、MCPでは、フラッシュメモリチップ6内に形成されたフラッシュメモリに対して外部(ライターなど)から書き込み、消去、読み出しなどが制御できる必要がある。このため、フラッシュメモリに対して入力信号“CE、WE、OE、ADDRESS、DATA”を外部から入力できる経路と、CPU4aを介して“CE、

WE、OE、ADDRESS、DATA”的入力を制御できる経路を設ける。

【0019】外部から“MODE”=“1”がMUX4b～4dのセレクト(S)端子に入力された場合、MUX4b～4dのA端子に入力された“CE、WE、OE、ADDRESS、DATA”がMUX4b～4dの出力(Z)端子からフラッシュメモリに供給される。

【0020】また、“MODE”=“0”がMUX4b～4dのセレクト(S)端子に入力された(CPUモード)場合、CPU4aからアドレスデコーダ4eを介してMUX4bのB端子に入力された“CE”が出力(Z)端子からフラッシュメモリに供給される。同様に、CPU4aからMUX4bのB端子に入力された“WE(WR)、OE(RD)”が出力(Z)端子からフラッシュメモリに供給され、CPU4aからMUX4c、4dのB端子に入力された“DATA、ADDRESS”が出力(Z)端子からフラッシュメモリに供給される。

【0021】次に、このMCPが有するセキュリティ機能について説明する。

【0022】CPUチップ4内に設けられたコンペアレジスタ4fにフラッシュメモリから第1のデータを入力し、外部から第2のデータを入力する。コンペアレジスタ4fは、第1のデータと第2のデータを比較して比較結果に応じた出力信号をトライステートバッファ4gに出力する。トライステートバッファ4gは、このコンペアレジスタ4fの出力信号が“1”か“0”かによりセキュリティ機能を働かせるか否かを切り換える。このセキュリティ機能の詳細は次のようにになっている。

【0023】まず、フラッシュメモリに予め記憶されているシグネチャコードがフラッシュメモリの第1端子から出力されて、コンペアレジスタ4fに入力される。また、外部からは入力コードが、MUX4cを介してコンペアレジスタ4fに入力される。

【0024】入力されたこれらのシグネチャコードと入力コードは、コンペアレジスタ4fにより比較され、一致した場合はコンペアレジスタ4fから“1”が出力される。コンペアレジスタ4fから出力された“1”がトライステートバッファ4gに入力されると、外部へのデータ出力が許可され、フラッシュメモリに記憶されているデータがこのトライステートバッファ4gを介して外部に出力される。

【0025】一方、シグネチャコードと入力コードが一致しない場合は、コンペアレジスタ4fから“0”が出力される。この“0”がトライステートバッファ4gに入力されると、外部へのデータ出力が禁止され、フラッシュメモリに記憶されているデータの出力はトライステートバッファ4fにより遮断される。

【0026】すなわち、フラッシュメモリに記憶されているシグネチャコードと外部から入力される入力コードがコンペアレジスタにより比較され、シグネチャコード

と入力コードが一致したときは外部へのデータ出力を有効とし、シグネチャコードと入力コードが一致しないときは外部へのデータ出力を禁止する。以上により、外部へのデータ出力を、正当なユーザに対しては許可し、不当なユーザに対しては禁止するというセキュリティ機能を実現する。

【0027】以上説明したようにこの実施の形態によれば、CPUチップにわずかな修正を加えることにより、すなわち、不揮発性メモリチップに予め記憶された参照用データと外部から入力される照合用データ（セキュリティ解除用データ）とを比較するコンペアレジスタと、このコンペアレジスタの比較結果に応じてデータの出力を許可状態に、あるいは禁止状態に切り換えるトライステイトバッファとを備えることにより、不揮発性メモリチップとCPUチップを1パッケージ化したMCPに対してセキュリティ機能を設けることができ、不揮発性メモリチップからデータが不正に読み出されるのを防止することができる。

【0028】

【発明の効果】以上述べたように本発明によれば、メモリチップとCPUチップを1つのパッケージに実装して

10

【符号の説明】

2…基板

4…CPUチップ

6…フラッシュメモリチップ

8、10、12、14…パッド

16…ボンディングワイヤ

4a…CPU

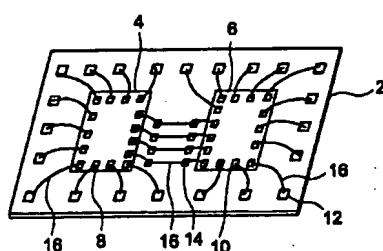
4b～4d…マルチプレクサ（以下MUX）

4e…アドレスデコーダ

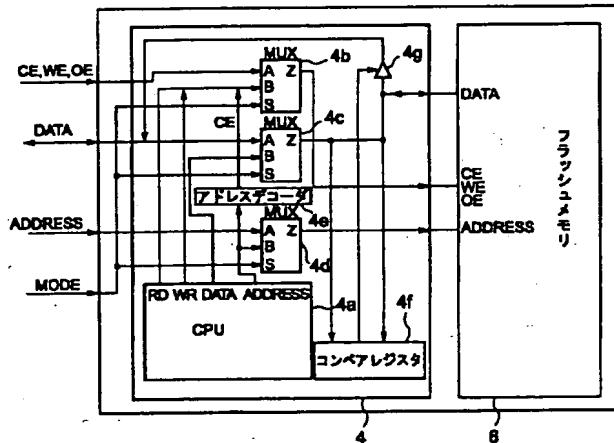
4f…コンペアレジスタ

20 4g…トライステイトバッファ

【図1】



【図2】



MCPを形成した半導体集積回路において、CPUチップのわずかな変更により、メモリチップに対してセキュリティ機能を設けることができる半導体集積回路を提供することが可能である。

【図面の簡単な説明】

【図1】この発明の実施の形態の半導体集積回路（MCP）の外観を示す概略図である。

【図2】この発明の実施の形態の半導体集積回路（MCP）MCPのブロックダイヤグラムを示す図である。

フロントページの続き

(51) Int.Cl.7

H 0 1 L 29/788
29/792

識別記号

F I

マークド(参考)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: _____**

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.